UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,563	02/18/2004	Venkatesh Veeraraghavan	50037.238US01	3537

27488 7590 08/20/2009

MERCHANT & GOULD (MICROSOFT)
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
GUPTA, MUKTESH G	

ART UNIT	PAPER NUMBER
2444	

MAIL DATE	DELIVERY MODE
08/20/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/782,563	VEERARAGHAVAN ET AL.	
	Examiner	Art Unit	
	Muktesh G. Gupta	2444	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 May 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-11,14-19,22 and 23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 7-11, 14-19 and 22-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1, 4, 7, 10, 14, 16, 18 and 22**are amended.

   Claims 6, 12-13 and 20-21 are cancelled.

   Claims 1-5, 7-11, 14-19 and 22-23 have been examined on merits and are pending in this application.

Response to Amendment

2. Acknowledgment is made for Applicants Amendments for claims filed on 05/11/2009.

   Applicants Amendment necessitated updating search and hence remapped grounds of rejections.

   Applicant's arguments with respect to pending claims have been considered but are moot in view of the remapped ground(s) of rejection.

   a. Applicant's arguments and amendments filed on 05/11/2009 have been carefully considered but they are deemed moot in view of the following remapped grounds of rejection as explained here below, necessitated by Applicant's substantial amendment to the claims "storing the received rules in a database; scheduling the compilation of the rules on a predetermined time schedule; independently generating separate results of the property query rule by determining if a property value matches a property of one or more of the plurality of users including receiving the separate results of the property

query rule from a directory service, wherein the directory service is separate from the database; which significantly affected the scope thereof.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. ***Claims 1-5, 7-11, 14-19 and 22-23*** *are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 6460141 to Olden; Eric M. (hereinafter "Olden").*

As to Claims 1, 10 and 16 Olden disclose method, system and computer program for targeting content to an audience that comprises a plurality of users, the method comprising (as stated in col. 4, lines 55-57, lines 1-6, lines 13-18, As shown in FIG. 1, the Web servers 20A, 20B, 20C provide Web-enabled applications and content to computer network users. Preferred configuration is as shown in FIG. 1, in which the security and access management system 10 comprises the plurality of authorization servers 24A, 24B, 24C and authorization dispatchers 26A, 26B, which operate in conjunction to provide efficient scalability of authorization requests. One of the authorization servers 24A, 24B, 24C communicates with an enabled Web server 20A,

20B, 20C and the authorization dispatchers 26A and 26B over a socket connection. The authorization servers 24A, 24B, 24C communicate with the entitlements server component 14 over a CORBA ORB (Object Request Broker)):

receiving rules from an administration client computing device, the rules comprising query criteria for the audience, each rule defined as a unit of functionality (as stated in col. 2, lines 66-67, col. 3, lines 1-2, lines 22-40, col. 7, lines 53-62, col. 8, lines 12-21, lines 44-50, FIG. 4 illustrates the data model architecture of the security and access management system for one embodiment of business rules to process user requests for access to application functions. Referring to FIG. 1A, When the Web server plug-ins are started, the plug-ins query the authorization dispatcher 26 for available authorization servers 24A, 24B, 24C. The plug-ins then starts querying the primary authorization server 24A, 24B, or 24C for authorization requests. The primary authorization server 24A, 24B, or 24C queries the entitlements database 32 for entitlements and responds to the requests from the plug-ins. An administrator defines a user 68 for each point of contact, adds each user 68 to a group 76 that represents the customer company, adds the group to a customer realm 78, and defines a user property 72, such as "service contract," of type integer. Then the administrator sets the service contract user property value for each user 68. As shown in FIG. 2, the access definition architecture 58 provides two approaches to assign access rights of a consumer or user 68 to a protected resource, namely, basic entitlements 80 or smart rules 82. Referring to FIG. 4, a smart rule 82 defines accessibility by specifying a criterion which a user property definition 72 for a user 68 must meet for the user to be granted access to an

application function 84. Smart rules 82 are expressions such as: "DENY if a property is less than a certain value". A user 68 is granted rights to an application 88. However, the security and access management system 10 actually does not assign rights at the application level, but assigns access rights to an application function 84. This is a powerful mechanism. Associating rules and rights at the application function level, instead of at the application level, provides greater security granularity. Smart rules 82 can also be strung together to form complex expressions. Smart rules can be used to automate the access privilege enforcement. A smart rule is defined that determines which properties (characteristics) of a user need be present in order to be given access);

storing the received rules in a database (as stated in col. 5, lines 13-15, col. 4, lines 27-33, col. 6, lines 53-62,In the preferred embodiment of the security and access management system 10, distributed authorization servers can run on NT and UNIX servers simultaneously. The entitlements (database) server component 14 performs database processing on behalf of at least one entitlements manager administrative client 18 and the API server 16. In addition, the entitlements server component 14 also forwards requests from the entitlements manager administrative client 18 and API server 16 to the authorization servers 24A, 24B, 24C comprising the authorization component 12. Security policy is defined using an access control architecture. Through the access control architecture, protected resources are associated with resource consumers, defining access control policy. Additionally, the security and access management system 10 provides a robust administration architecture, securing access

to the entitlements database 32. Through the administration architecture, a user is associated with administrative rights and ownership, defining an administrative policy);

scheduling the compilation of the rules on a predetermined time schedule (as stated in *col. 19, lines 3-15,* Smart rules essentially build access control lists dynamically based on the properties of the users. The properties of a user are such things as "job title" or "account balance" or "premium account holder" or "trustee." Properties are nouns which are used in day-to-day business operations. These properties most often reside in existing enterprise databases, such as customer list databases or employee databases. In order for a smart rule to operate against a particular property, the smart rule must first be defined in the entitlements database 32. Then, the properties from the customer or employee database can be loaded into the entitlements database 32, and synchronized periodically to keep them up to date. This can be easily done through the bulk loading function of the API server 16. Once the user properties have been extended and populated, the process of building smart rules begins. These smart rules are dynamic, since they are applied to properties which are continually updated through the bulk loading function);

using the received rules to determine a membership list of the plurality of users to receive the content, the received rules comprising a property query rule, a member of rule, and a reports under rule, by (as stated in col. 8, lines 52-67, col. 9, lines 1-34, col. 13, lines 23-49, col. 17, lines 14-26, lines 66-67, col. 18, lines 1-10, lines 35-37, lines 59-63, The ACCESS function is used by enabled Web server objects 92 to determine access rights of a user 68 to an application 88. However, an administrator can add

additional application functions 84 to the application 88 through the API client 22. The additional application functions 84 can further define whether or not a user 68 has privileges to use various services associated with an application 88. The access rights to these additional application functions 84 can be determined through the API server 16. For a Web-based application 88, the application can contain URIs 90. Associated with a URI 90 is a defined Web server object 92 which owns the URI. Together, the URI 90 and Web server object 92 combine to form a Uniform Resource Locator (URL). The Web server object 92, besides identifying the location of a URI 90, also defines the identity of an enabled Web server 20 shown in FIG. 1. Thus, when a URL is requested from an enabled Web server 20, both the URI 90 shown in FIG. 2 of the requested URL and the identity of the enabled Web server define the application 88 being referenced. The ACCESS application function 84 of the referenced application 88 is used for determining accessibility to the requested URL. For example, consider the situation in which a customer account application has varying functionality depending on the service contracts with customers. Consequently, a service contract provider wants all of its customers to be able to access the customer account application, but return an interface supporting only the level of functionality that matches the service contract of the customer. In order to accomplish this, an administrator of the service contract service provider would create an application 88, for example, denoted CustomerAccountApplication. Next, the administrator would define the URI 90 of the application 88, /customeraccountapp.cgi, and a Web server object 92 which owns the application, for example, WebServer. The administrator would then define application

functions 84 representing the various functionality of the CustomerAccountApplication. The administrator associates either a basic entitlement 80 or a smart rule 82 with the ACCESS application function 84 and each additionally defined application function. During a request for the CustomerAccountApplication, the enabled Web server 20 processes the ACCESS application function 84 to determine accessibility to the application 88. Once a user 68, that is, a service contract customer, is granted access, the customer account application uses the API server 16 to determine the different application functions 84 to which the customer has access rights, and returns the correct interface which supports the function set. The security and access management system 10 allows a security administrator to create an unlimited number of users, each with individual defining properties. The administrator can further collect users into groups and groups into realms. Additionally, users can be in multiple groups. This feature is useful for administrators trying to mimic organizational structure (for example, user John Doe may be in the promotions group, which is in the marketing realm) or geography (user Jane Doe is in the Paris group, which is in the Europe realm), or any other type of grouping. The user/group/realm concept is also important for setting permissions and entitlements, as described in connection with the description of the Basic Entitlements page. Entitlements are defined and administered using the Basic Entitlements page, as shown in FIG. 17. By adding entitlements using the security and access management system 10, entitlements to particular applications can be assigned to users, groups, or realms with ease. First, the administrator selects the user, group, or realm to be granted the entitlement. This is similar to the selection process on the Users

page, described earlier. The appropriate entity is then selected from the entity menu. Clicking the left Choose button brings up a list of all available users, groups, or realms. The entity to be administered is selected from this list, and the Choose button is clicked. All of the entitlements for the selected user, group, or realm appear in the Basic Entitlements list box. Smart rules are filters that govern user access to applications. When a smart rule is defined for an application, in order to determine authorization, the security and access management system 10 examines a property for a specific user, and grants or denies access to an application resource based on the value that is found. The smart rules filter box shown in FIG. 19 is employed to create a filter. A filter comprises four components, namely, a rule type, a property, an operator, and a Value. Once the property and operator are selected, a value must be entered into the Value field. The security and access management system 10 only accepts valid values based on the property type. All of this information combines to create a smart rule);

independently generating separate results of the property query rule by determining if a property value matches a property of one or more of the plurality of users including receiving the separate results of the property query rule from a directory service, wherein the directory service is separate from the database; (as stated in col. 13, lines 37-49, col. 14, lines 33-49, col. 30, lines 7-29, In order to find a particular user, group, or realm in the list box, an administrator can scroll through the list of entities or use the Search function. The Search function is indexed differently depending on the type of entity selected. For users, the Search function indexes on last name. For groups and realms, the Search function indexes on the group or realm name. In order to add

users to a group, Users is selected in the entity menu. The user list appears in the entity list box. In order to set a property for a new user, the user is selected from the User list, and the Modify button is clicked to bring up the Modify User dialog window which is similar to the Create User window shown in FIG. 9, but contains the information that was entered when the user was created. The Property list contains all of the properties available for the selected user. In order to change a property Value, the Property is selected, and the Change Property Value button is clicked. The Enter Property dialog window then appears. A value can be entered for the property. The security and access management system 10 only allows valid property values to be entered, based on the property type (True or False for Boolean properties, integers for integer properties, real numbers for floating-point properties, dates for date properties, character strings for string properties, and null for properties that can be set to null. The security and access management system 10 can leverage data that resides in an LDAP directory like other LDAP-enabled applications. By leveraging the LDAP directory data, organizations can centrally manage user information in the directory and use the security and access management system 10 to define security policy and to secure Web resources. security and access management system 10 provides a Web security system that combines native LDAP support with powerful Oracle database scalability. This combination of the security and access management system 10 and LDAP provides many benefits and enables: 1) companies to use an LDAP directory server to centrally store and manage user information, such as passwords, e-mail addresses, contract numbers, and other common user attributes; 2) companies to use multiple LDAP directory servers; 3) Web

applications to incorporate users' LDAP attributes (properties) to dynamically generate personalized Web pages; and 4) Business to business application and data integration across firewalls via LDAP. Business Rules--Secure Rules--Smart Rules Data driven meanings are driven from data about a user, both individually and at group level. Rules are executed against data about a user that is dynamic; therefore access control decisions can be automated. Because the rule system can access up-to-date information without administration intervention, the changes that affect the user (credit or sales volume) automatically affect the user's access privileges. Rules can be grouped together using "and" and "or" operators Rules can be ordered in terms of Allow before Deny Rule operators reflect data type of the user property--date data type has date operators "before" and "after" Rules can be driven off of LDAP attributes Rules can be applied to both the ACCESS control function, as well as f(n) not access Rules are driven at runtime and are dynamic Data that is evaluated can be driven off of internal data, as well as external data Supports various data types: integer, Boolean, date, string, float Rules can be applied to grouping of roles--must be "Role A and Role B but not Role C" Rules can be driven externally and included in decisions);

independently generating separate results of the a member of rule by determining if one or more of the plurality of users are a member of a group email distribution list (as stated in col. 10, lines 40-47, col. 15, lines 12-19, col. 17, lines 32-38, User means a single user of Web applications protected by the security and access management system 10, using various user properties such as username, password, e-mail address, IP address, etc. Group means a collection of users, grouped together for

ease of administration. Groups have specific properties. A realm is a collection of groups. A realm contains all of the users within the component groups of the realm. Entity means a user, group, or realm. In order to add users to a group, Users is selected in the entity menu. The user list appears in the entity list box. Then, the Select Group button is clicked. The Group List dialog window will appear. The group to be populated is then selected, and the OK button is clicked. In order to include users in that group, the user to be added is highlighted to select the user, and the Add Arrow button is then clicked. In order to grant a Basic Entitlement to the selected user, group, or realm, the appropriate application function is highlighted, and the Left Arrow button is clicked. The application name, function name, and default entitlement setting (Allow or Deny) will then appear in the Basic Entitlements list box for the user);

and independently generating separate results of the a reports under rule by determining if one or more of the plurality of users are located hierarchically under another person within an organization structure, the determination comprising receiving the separate results of the reports under rule from the directory service maintaining the organization structure; (as stated in col. 7, lines 42-48, col. 9, lines 35-62, col. 10, lines 62-67, col. 11, lines 1-15, col. 15, lines 26-46, col. 21, lines 15-21, The resource consumer architecture 56 also provides a containment hierarchy or containers 74 of users 68. This allows an administrator to more easily assign access rights to a large group of users 68 without having to assign rights individually. A user 68 can be grouped together into a group object 76. Group objects 76 likewise can be grouped together into a realm object 78. Finally, as shown in FIG. 2, the administrative architecture 54

provides a flexible model for defining ownership and administrative responsibilities of data model architecture objects. On the one hand, ownership can be used to segment objects by their geographical location, organizational structure, or other logical grouping to limit access by an administrator to only objects in his or her area of responsibility. An area of ownership is defined as an administrative group 94. For example, an administrator can be defined that can modify only objects in the North American Administrative Group. Consider the following example. A company is using the security and access management system 10 to protect its external customer account application, but it is protecting its internal human resource (HR) information as well. In order to manage administration of the entitlements database 32, the company can define two administrative groups 94, namely, Customer Administrative Group and HR Administrative Group. Next, the company can define two administrative roles 96, Customer Admin Role and HR Admin Role, granting each administrative role a full set of administrative privileges. An entitlement is a relationship between an entity and an application. An entitlement gives a user access to an application on the Web. An administrator is an individual who creates and maintains entities, applications, and entitlements on the intranet. In comparison, a sub-administrator is a type of user that can perform limited administrative tasks via the security and access management system 10, as designated by the administrator. An administrative group is a set of ownable resources that is configured to be under the control of a particular set of administrators. Administrative role means a role defining the types of operations an administrator can perform on a particular administrative group. An ownable resource is

one of all of the types of resources defined in the security and access management system 10, which can fall under the control of an administrative group. They are: user, group, realm, application, Web server, administrative roles, and user property definitions. Other resources, such as entitlements and smart rules, are owned by default by the group that owns the related application, property, or user/group/realm. Adding groups to realms and removing groups from realms is similar. When Groups is selected in the entity menu, the Select Group button automatically changes to read Select Realm. The Select Realm button is clicked, and the realm to be changed is selected from the realm list dialog window. In order to add a group to that realm, the group to be added is highlighted to select the group, and the Add Arrow button is clicked. In order to delete a group from the realm, the group to be removed is highlighted to select the group, and the Remove Arrow button is clicked. In order to edit a user, group, or realm, Users, Groups, or Realms is selected from the entity menu. All of the available entities of that type then appear in the list box below. The user, group, or realm to be modified is then highlighted to select the entity, and then the Modify button is clicked. The Modify dialog window appears. The Modify dialog window is identical to the Create dialog window, but contains all of the current user/group/realm information, which can be edited. Once the fields in the Modify dialog window have been changed, OK is clicked to complete the Modify, or the Cancel button is clicked to abort. An enterprise can create a hierarchical administration structure which allows for a grandparent.fwdarw.parent.fwdarw.child.fwdarw.grandchild type structure. Additionally,

the enterprise can avoid being in the business of administration and is able to push administration of additional groups down the administration chain);

and after independently generating the separate results of each of the property query rule, the member of rule, and the reports under rule, compiling the membership list of users according to the predetermined schedule by applying one or more conditional logic operators to combine the separate results of the property query rule, the separate results of the member of rule, and the separate results of the reports under rule; associating the compiled membership list of users with content (as stated in col. 18, lines 21-56, col. 19, lines 12-28, Various steps are required to create a smart rule. Referring to FIG. 18, the first step in creating a smart rule is selecting the Application for which the smart rule is to be created. The application list will disappear, and all of the application functions for the selected application will appear in the Application Functions list box. The function to which the smart rule is to apply is then selected. From the User Properties list box, the user property to be examined is selected. In order to create the entitlement, the Left Arrow button is clicked. This brings up the smart rules filter box, as shown in FIG. 19. The smart rules filter box shown in FIG. 19 is employed to create a filter. A filter comprises four components, namely, a rule type, a property, an operator, and a Value. The rule is selected from the rule list, which is a pull-down list beside the word Define. As described above, the rule is either Require, Deny, or Allow. The property is the property selected on the smart rules main page shown in FIG. 18. The operator is selected from the operator pull-down menu. The available operators depend on the type of property. Integer properties (INT) have mathematical operators, such as >

(greater than); <(less than); = (equal to) ;!=(not equal to); >= (greater than or equal to); and <=(less than or equal to). Floating-point properties (FLOAT) have the following mathematical operators: > (greater than); <(less than); = (equal to) ;!=(not equal to); >= (greater than or equal to); and <=(less than or equal to). Boolean properties (BOOL) are either True or False. Their operators are IS or IS NOT. String properties (STRING) have the following operators: Contains, Does Not Contain, Ends With, Starts With, and Equals. Finally, date properties (DATE) have two operators, namely, BEFORE and AFTER. The BEFORE and AFTER properties are not inclusive. Smart rules essentially build access control lists dynamically based on the properties of the users. These properties most often reside in existing enterprise databases, such as customer list databases or employee databases. In order for a smart rule to operate against a particular property, the smart rule must first be defined in the entitlements database 32. Then, the properties from the customer or employee database can be loaded into the entitlements database 32, and synchronized periodically to keep them up to date. This can be easily done through the bulk loading function of the API server 16. Once the user properties have been extended and populated, the process of building smart rules begins. These smart rules are dynamic, since they are applied to properties which are continually updated through the bulk loading function);

obtaining the content from a data store (as stated in col. 24, lines 1-13, col. 16, lines 1-26, lines 51-59, Referring to FIG. 30, the single sign on process is as follows. 1) The browser requests secured content from protected Web server 20A. 2) The plug-in for Web server 20A checks for a cookie. 3) Because this is the first authentication, the

user provides his or her username and password. 4) User permissions are checked. 5) A cookie is built and set for the browser. 6) The Web user accesses protected Web server 20B. 7) The plug-in for Web server 20B uses the cookie for authentication. 8) Permissions are checked for the user based on the user's credentials contained in the cookie. Referring to FIG. 16, the Applications page is employed for administrators to define the Web applications available to users of the security and access management system 10. Each application is comprised of an unlimited number of resources. Each resource is defined as a particular Web "page" or URI. Thus, an application can have one resource devoted to calculation, one to printing, one to saving, etc. The Applications page shown in FIG. 16 is also used to create application privileges. These privileges are most easily explained by example. The most basic application privilege is access. If a user has the access privilege granted for a certain application, he or she can navigate to that application on the intranet. Otherwise, the security and access management system 10 does not allow the user to access that application. Every application has the access entitlement by default. Other application entitlements can control other aspects of the functionality of the application. An application can have a print entitlement, or a save entitlement, for example. The user can be allowed to download appropriate applets based on permissions managed by the security and access management system 10. Application entitlements dictate the level of control that the administrator has over application access. Applications with only the access entitlement are completely available to anyone with that entitlement. Applications with entitlements for each of their various functions allow finer-grained control. As described

earlier, resources are the component parts of each application. Referring to FIG. 16, clicking the Add button above the Resources window brings up the Create Resource dialog window. There are two ways to define a resource. One option is to enter a complete resource URI (/hr/benefits/copay/lookup.html, for example). The other is to use wildcards (/hr/benefits/copay/*.html or /hr/benefits/*). The resource must also be associated with a Web server 20 defined using the Web Servers page.

and providing the content to the users listed within the compiled membership list. (as stated in col. 17, lines 66-67, col. 18, lines 1-4, Smart rules are filters that govern user access to applications and content. When a smart rule is defined for an application, in order to determine authorization, the security and access management system 10 examines a property for a specific user, and grants or denies access to an application resource based on the value that is found).

As to Claims 2, 11 and 17 *Olden disclose method, system and computer program of Claims 1, 10 and 16, wherein the rules to define the audience further comprises an attribute (as stated in col. 7, lines 26-41,* Specifically, as shown in FIG. 2, the resource consumer architecture 56 comprises a consumer architecture which is divided into a consumer object model 64 and an extensible consumer attribute model 66. A consumer object is referred to as a user 68. A user 68 has several defined attributes (for example, user ID, first name, last name, password, etc.), as well as extendible attributes. These extendible attributes are referred to as user properties 70. The name and type of a user property 70 (for example, a string property, a date

property, and integer property, etc.) is defined by a user property definition 72. When a user property definition 72 is created, all users 68 automatically inherit a user property 70 of the defined name and type. However, a value is not automatically assigned to a user property 70. A user property definition 72 preferably includes at least one of the following types: Boolean; string; integer; floating point; and date);

a member; and an organization (as stated in col. 7, lines 42-48, The resource consumer architecture 56 also provides a containment hierarchy or containers 74 of users 68. This allows an administrator to more easily assign access rights to a large group of users 68 without having to assign rights individually. A user 68 can be grouped together into a group object 76. Group objects 76 likewise can be grouped together into a realm object 78).

As to Claims 3, 15 and 23 *Olden disclose method, system and computer program of Claims 1, 10 and 16, wherein the content is provided within a web part (as stated in col. 7, lines 11-48, col. 8, lines 34-43,* a resource consumer is someone who accesses or manipulates a defined resource. Generally, a resource consumer is someone who requests access to a Web-enabled or non-Web-enabled application or content. For example, a resource consumer could be an employee who needs to retrieve sensitive documents, a customer who wishes to modify his or her account information, or a supplier with rights to view. Referring again to FIG. 2, the resource definition architecture 60 comprises an application architecture 86 which groups protected resources into applications 88. A Web-based application 88 is comprised of

Uniform Resource Identifiers (URIs) 90. Other types of applications do not have resources directly contained in the application; rather, the application represents implicitly a group of resources. Applications 88 also have associated application functions 84, which represent the various services associated with an application).

As to Claims 4-5 and 19 *Olden disclose method and computer program of Claims 1 and 16, wherein an organization structure is stored in the directory service (as stated in col. 12, lines 18-36, col. 13, lines 23-29, col. 29, lines 59-67,* The operation of the administrative client 18 shown in FIG. 1 the entitlements manager software for the security and access management system 10 is launched, which causes a login window to be displayed, as shown in FIG. 6. In the case that the security and access management system 10 is running on a Windows 95/NT platform, there are two options to launch the entitlements manager. The first option is to select an entitlements manager icon from the start menu.fwdarw.programs. The second option is to double click a clrtrustmgr.bat file under the directory for the entitlements manager for the security and access management system 10. The security and access management system 10 allows a security administrator to create an unlimited number of users, each with individual defining properties. The administrator can further collect users into groups and groups into realms. Additionally, users can be in multiple groups. This feature is useful for administrators trying to mimic organizational structure. Finally, an LDAP directory is an effective way to store commonly shared organization information that can be accessed using standard Internet protocols. Because of its centralized,

platform and vendor independent design, it is ideal to leverage LDAP into the Web security infrastructure. However, while LDAP directories provide excellent centralized data repository and access functionality, they do not provide tools for defining, managing, and deploying Web security policy).

As to Claims 7, 14 and 22 *Olden disclose method, system and computer program of Claims 1, 10 and 16, wherein scheduling the compilation of the rules on a predetermined time schedule is processed as a SQL job by the database and scheduled by the database (as stated in col. 19, lines 12-28, col. 29, lines 9-20, col. 30, lines 14-29,* Smart rules essentially build access control lists dynamically based on the properties of the users. The properties of a user are such things as "job title" or "account balance" or "premium account holder" or "trustee." Properties are nouns which are used in day-to-day business operations. These properties most often reside in existing enterprise databases, such as customer list databases or employee databases. In order for a smart rule to operate against a particular property, the smart rule must first be defined in the entitlements database 32. Then, the properties from the customer or employee database can be loaded into the entitlements database 32, and synchronized periodically to keep them up to date. This can be easily done through the bulk loading function of the API server 16. Once the user properties have been extended and populated, the process of building smart rules begins. These smart rules are dynamic, since they are applied to properties which are continually updated through the bulk loading function. A data server log file, CT_Dataserver.log, preferably records all errors

that occur during runtime operation of the entitlements server 14, including all SQL-related errors. Automatic rotation of the data server log file preferably occurs when the log file reaches a predetermined size, for example, five megabytes. The data server log file will typically grow over time, because some SQL errors are a result of normal operation. In a preferred embodiment, the security and access management system 10 provides a Web security system that combines native LDAP support with powerful Oracle database (or SQL database) scalability. This combination of the security and access management system 10 and LDAP provides many benefits and enables: 1) companies to use an LDAP directory server to centrally store and manage user information, such as passwords, e-mail addresses, contract numbers, and other common user attributes; 2) companies to use multiple LDAP directory servers, including those from Netscape or Novell; 3) Web applications to incorporate users' LDAP attributes to dynamically generate personalized Web pages; and 4) Business to business application and data integration across firewalls via LDAP.).

As to Claim 8 *Olden disclose method of Claim 1, further comprising providing access to the content through a web interface that is created individually for that audience member (as stated in col. 24, lines 1-13,* Referring to FIG. 30, the single sign on process is as follows. 1) The browser requests secured content from protected Web server 20A. 2) The plug-in for Web server 20A checks for a cookie. 3) Because this is the first authentication, the user provides his or her username and password. 4) User permissions are checked. 5) A cookie is built and set for the browser. 6) The Web

user accesses protected Web server 20B. 7) The plug-in for Web server 20B uses the cookie for authentication. 8) Permissions are checked for the user based on the user's credentials contained in the cookie).

As to Claim 9 *Olden disclose method of Claim 1, further comprising storing the rules to define the audience as an XML representation (as stated in col. 22, lines 48-61,* A user property can also be modified. After selecting the property to be modified, clicking the Modify button on the User Properties page shown in FIG. 26 brings up a Modify User Property dialog window. This window is identical to the Create User Property dialog window shown in FIG. 27, but the details of the selected user property are included and can be edited. Once the user property has been changed as needed, clicking the Save button saves the changes, and clicking the Cancel button aborts. Some characteristics of the property, specifically Owner, can only be changed by administrators with special permissions (specifically, the ability to Modify Ownership, set on the Administrators page). User Properties can only be set for existing users, by modifying that user on the Users Page).

As to Claim 18 *Olden disclose computer storage medium of Claim 16, wherein gathering information from the organization structure comprises invoking a directory service rules compiler. (as stated in col. 13, lines 37-49, col. 14, lines 33-49, col. 30, lines 7-29,* In order to find a particular user, group, or realm in the list box, an administrator can scroll through the list of entities or use the Search function. The

Search function is indexed differently depending on the type of entity selected. For users, the Search function indexes on last name. For groups and realms, the Search function indexes on the group or realm name. In order to add users to a group, Users is selected in the entity menu. The user list appears in the entity list box. In order to set a property for a new user, the user is selected from the User list, and the Modify button is clicked to bring up the Modify User dialog window which is similar to the Create User window shown in FIG. 9, but contains the information that was entered when the user was created. The Property list contains all of the properties available for the selected user. In order to change a property Value, the Property is selected, and the Change Property Value button is clicked. The Enter Property dialog window then appears. A value can be entered for the property. The security and access management system 10 only allows valid property values to be entered, based on the property type (True or False for Boolean properties, integers for integer properties, real numbers for floating-point properties, dates for date properties, character strings for string properties, and null for properties that can be set to null. The security and access management system 10 can leverage data that resides in an LDAP directory like other LDAP-enabled applications. By leveraging the LDAP directory data, organizations can centrally manage user information in the directory and use the security and access management system 10 to define security policy and to secure Web resources. security and access management system 10 provides a Web security system that combines native LDAP support with powerful Oracle database scalability. This combination of the security and access management system 10 and LDAP provides many benefits and enables: 1)

companies to use an LDAP directory server to centrally store and manage user information, such as passwords, e-mail addresses, contract numbers, and other common user attributes; 2) companies to use multiple LDAP directory servers; 3) Web applications to incorporate users' LDAP attributes (properties) to dynamically generate personalized Web pages; and 4) Business to business application and data integration across firewalls via LDAP. Business Rules--Secure Rules--Smart Rules Data driven meanings are driven from data about a user, both individually and at group level. Rules are executed against data about a user that is dynamic; therefore access control decisions can be automated. Because the rule system can access up-to-date information without administration intervention, the changes that affect the user (credit or sales volume) automatically affect the user's access privileges. Rules can be grouped together using "and" and "or" operators Rules can be ordered in terms of Allow before Deny Rule operators reflect data type of the user property--date data type has date operators "before" and "after" Rules can be driven off of LDAP attributes Rules can be applied to both the ACCESS control function, as well as f(n) not access Rules are driven at runtime and are dynamic Data that is evaluated can be driven off of internal data, as well as external data Supports various data types: integer, Boolean, date, string, float Rules can be applied to grouping of roles--must be "Role A and Role B but not Role C" Rules can be driven externally and included in decisions).

Response to Arguments

4. Applicant's arguments filed 05/11/2009 have been fully considered but they are not persuasive.

a. Regarding Olden Does Not Teach Receiving Property Query and Reports Under Rule Results from a Separate Directory Service

Olden discloses as stated in col. 19, lines 12-28, col. 29, lines 59-67, Smart rules essentially build access control lists dynamically based on the properties of the users. In order for a smart rule to operate against a particular property, the smart rule must first be defined in the entitlements database 32. Then, the properties from the customer or employee database can be loaded into the entitlements database 32, and synchronized periodically to keep them up to date. LDAP directory is an effective way to store commonly shared organization information that can be accessed using standard Internet protocols. Because of its centralized, platform and vendor independent design, it is ideal to leverage LDAP into the Web security infrastructure. However, while LDAP directories provide excellent centralized data repository and access functionality.

b. Regarding Olden Does Not Teach a Member OF Rule for a Group Email Distribution List.

Olden discloses as stated in col. 10, lines 40-47, col. 15, lines 12-19, col. 17, lines 32-38, User means a single user of Web applications protected by the security and access management system 10, using various user properties such as username, password, e-mail address, IP address, etc.

Group means a collection of users (having property, such as belonging to email distribution list) grouped together for ease of administration. Groups have specific properties. A realm is a collection of groups. A realm contains all of the users within the component groups of the realm. Entity means a user, group, or realm. In order to add users to a group, Users is selected in the entity menu. The user list appears in the entity list box. Then, the Select Group button is clicked. The Group List dialog window will appear. The group to be populated is then selected, and the OK button is clicked. In order to include users in that group, the user to be added is highlighted to select the user, and the Add Arrow button is then clicked. In order to grant a Basic Entitlement to the selected user, group, or realm, the appropriate application function is highlighted, and the Left Arrow button is clicked. The application name, function name, and default entitlement setting (Allow or Deny) will then appear in the Basic Entitlements list box for the user.

c. Regarding Olden Does Not Teach a Reports Under Rule

Olden discloses as stated in col. 7, lines 26-48, as shown in FIG. 2, the resource consumer architecture 56 comprises a consumer architecture which is divided into a consumer object model 64 and an extensible consumer attribute model 66. A consumer object is referred to as a user 68. A user 68 has several defined attributes (for example, user ID, first name, last name, password, etc.), as well as extendible attributes. The

resource consumer architecture 56 also provides a containment hierarchy or containers 74 of users 68. This allows an administrator to more easily assign access rights to a large group of users 68 without having to assign rights individually. A user 68 can be grouped together into a group object 76. Group objects 76 likewise can be grouped together into a realm object 78. Furthermore, administrative groups can be nested. For example, an enterprise can create a hierarchical administration structure which allows for grandparent.fwdarw.parent.fwdarw.child.fwdarw.grandchild type structure. Additionally, the enterprise can avoid being in the business of administration and is able to push administration of additional groups down the administration chain.

d. Regarding Olden Does Not Teach Combining Results Returned by the Property 0uery Rule, the Member of Rule and the Reports Under Rule

Olden discloses as stated in col. 8, lines 52-67, col. 9, lines 1-34, col. 13, lines 23-49, col. 17, lines 14-26, lines 66-67, col. 18, lines 1-10, lines 35-37, lines 59-63, The ACCESS function is used by enabled Web server objects 92 to determine access rights of a user 68 to an application 88. However, an administrator can add additional application functions 84 to the application 88 through the API client 22. The additional application functions 84 can further define whether or not a user 68 has privileges to use various services associated with an application 88. The administrator associates either a basic entitlement 80 or a smart rule 82 with the

ACCESS application function 84 and each additionally defined application function. The security and access management system 10 allows a security administrator to create an unlimited number of users, each with individual defining properties. The administrator can further collect users into groups and groups into realms. Additionally, users can be in multiple groups. This feature is useful for administrators trying to mimic organizational structure. The user/group/realm concept is also important for setting permissions and entitlements, as described in connection with the description of the Basic Entitlements page. Entitlements are defined and administered using the Basic Entitlements page, as shown in FIG. 17. By adding entitlements using the security and access management system 10, entitlements to particular applications can be assigned to users, groups, or realms with ease. First, the administrator selects the user, group, or realm to be granted the entitlement. This is similar to the selection process on the Users page, described earlier. The appropriate entity is then selected from the entity menu. Clicking the left Choose button brings up a list of all available users, groups, or realms. The entity to be administered is selected from this list, and the Choose button is clicked. All of the entitlements for the selected user, group, or realm appear in the Basic Entitlements list box. Smart rules are filters that govern user access to applications. When a smart rule is defined for an application, in order to determine authorization, the security and access

management system 10 examines a property for a specific user, and grants or denies access to an application resource based on the value that is found. The smart rules filter box shown in FIG. 19 is employed to create a filter. A filter comprises four components, namely, a rule type, a property, an operator, and a Value. Once the property and operator are selected, a value must be entered into the Value field. The security and access management system 10 only accepts valid values based on the property type. All of this information combines to create a smart rule.

Hence arguments are not persuasive and are moot in view of the remapped ground(s) of rejection.

Action Final

5. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Muktesh G. Gupta whose telephone number is 571-270-5011. The examiner can normally be reached on Monday-Friday, 8:00 a.m. -5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William C. Vaughn can be reached on 571-272-3922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MG

/LaShonda T Jacobs/

Primary Examiner, Art Unit 2457